Groupes

Mohamed Talbi et Mohammed Talbi

Centre régional des métiers de l'éducation et de la formation

2017-2018

Définition (Loi de composition interne)

Une loi de composition interne sur un ensemble E *est la donnée d'une application de* $E \times E \rightarrow E$*. Plutôt que loi de composition interne on dit aussi opération.*
L'image du couple $(u,v) \in E \times E$ *par cette application est notée généralement* $u*v$, uTv, $u.v$, $u+v$ *etc, et on parle alors des lois* $*$, T, $\cdot$, $+$, *etc.*
On note souvent par $(E,*)$ *pour désigner un ensemble* E *muni d'une loi de composition interne "*$*$*".*

Exemple

1) *Les opérations "+" et "×" sont des lois de composition internes sur* $\mathbb{Z}$, $\mathbb{Q}$ *et* $\mathbb{R}$.
2) *Les lois* $\cap$ *(intersection) et* $\cup$ *(union) sont des lois de composition internes sur* $\mathcal{P}(E)$ *(ensemble des parties de* E*).*
3) *Soit* $(E,*)$ *un ensemble muni d'une loi de composition interne, et soit* X *un ensemble, on définit une loi, notée encore "∗", sur l'ensemble* $\mathcal{F}(X,E)$ *des applications de* E *dans* X*, en posant :*

$$\forall (f,g) \in \mathcal{F}(X,E)^2, \forall x \in X,\ (f*g)(x) = f(x)*g(x).$$

Ce qui nous permet de définir des lois "+" et "×" sur l'ensembles des applications de X *vers* $\mathbb{R}$ *(ou* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$*).*
Si $X = \mathbb{N}$*, on définit ainsi la loi "∗" sur l'ensemble des suites de* E*.*

Définition (Partie stable par une loi)

Soient $(E, *)$ *un ensemble muni d'une loi de composition interne* $*$ *et* F *une partie de* E. *On dit que* F *est stable par la loi* $*$, *si*

$$\forall(x,y) \in F,\ x * y \in F.$$

La restriction à $F \times F$ *de la loi "*$*$*" définit alors une loi de composition interne sur F, appelée loi induite et généralement noté "*$*$*".*

Dans toute la suite (sauf mention contraire) une loi de composition interne sera notée par "." multiplicativement ou "+" additivement.

Définition (Groupe)

Soit G *un ensemble muni d'une loi de composition interne* $(x,y) \mapsto x.y$*. On dit que* $(G,.)$ *est un groupe (ou muni d'une structure de groupe) si les conditions suivantes sont vérifiées :*

1) *La loi "." est associative, c.-à-d.*

$$(\forall\ x,y,z \in G),\ (x.y).z = x.(y.z).$$

2) *La loi "." admet un élément neutre, c.-à-d.*

$$(\exists\ e \in G), (\forall\ x \in G),\ x.e = e.x = x.$$

3) *Tout élément* $x \in G$ *admet un symétrique* $x' \in G$ *pour la loi ".", c.-à-d.*

$$(\forall\ x \in G), (\exists\ x' \in G) :\ x.x' = x'.x = e.$$

Le groupe $(G,.)$ *est dit commutatif (ou abélien), si la loi "." est commutative, c.-à-d.*

$$\forall (x,y) \in G^2,\ x.y = y.x.$$

Remarque

1) *Lorsque la loi est notée multiplicativement on écrit* $x.y$ *ou tout simplement* xy.
2) *Si la loi est notée multiplicativement, on note par "*1*" l'élément neutre de* G *et l'inverse d'un élément* x *est noté* x^{-1}.
3) *Si la loi est notée additivement, on note par '*0*" l'élément neutre de* G *et l'inverse d'un élement* x *est noté* $-x$.

Propriétés

Soit $(G, .)$ *un groupe alors on a :*

1) G *est non vide.*

2) *L'élément neutre de* G *est unique.*

3) *Si* $x \in G$*, l'inverse de* x *dans* G *est unique.*

Propriétés

Soit $(G,.)$ un groupe alors on a :

1) *G est non vide.*
2) *L'élément neutre de G est unique.*
3) *Si $x \in G$, l'inverse de x dans G est unique.*

Preuve.

1) $G \neq \emptyset$ car l'élément neutre e appartient à G.
2) Si e' un autre élément neutre de G alors $e' = ee' = e'e = e$.
3) soit $x \in G$. Si x' et x'' deux inverses de x dans G alors on a

$$x' = x'e = x'xx" = ex" = x".$$



Exemple

1) *Les ensembles* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ *muni de l'addition sont des groupes commutatifs.*
2) $(\mathbb{N},+)$, $(\mathbb{Z}^*,.)$ *ne sont pas des groupes.*
3) *Les ensembles* $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $(\mathbb{Z}/n\mathbb{Z})^\times$ *muni de la multiplication sont des groupes commutatifs.*
4) *L'ensemble des matrices carrées inversibles noté* $GL_n(\mathbb{R})$ *muni de la loi "*$\times$*" est un groupe non commutatif.*
5) *Soit* E *un ensemble non vide, alors l'ensemble des applications bijectives de* E *vers lui même, noté* $\mathcal{S}(E)$*, muni de la loi de composition d'applications "*$\circ$*" est un groupe non commutatif. En particulier si* $E = \{1,2,\ldots,n\}$*, l'ensemble* $\mathcal{S}(E)$ *est noté* $\mathcal{S}_n$ *s'appelle le groupe symétrique (ou le groupe des permutations).*

Définition

Soient $(G,.)$ *un groupe,* e *son élément neutre et* a *un élément de* G*.*

- *Pour* $n \in \mathbb{N}$ *on définit l'élément* a^n *par* $a^0 = e$, $a^{n+1} = a^n.a = a.a^n$.
- *Pour* $n \in \mathbb{Z}^-$ *on définit l'élément* a^n *par* $a^n = (a^{-1})^{-n}$.

Définition

Soient $(G,.)$ *un groupe,* e *son élément neutre et* a *un élément de* G.

- *Pour* $n \in \mathbb{N}$ *on définit l'élément* a^n *par* $a^0 = e$, $a^{n+1} = a^n.a = a.a^n$.
- *Pour* $n \in \mathbb{Z}^-$ *on définit l'élément* a^n *par* $a^n = (a^{-1})^{-n}$.

Propriétés

Soit $(G,.)$ *un groupe alors on a :*

1) G *est régulier à gauche c.-à-d.* $\forall a \in G$, $\forall x,y \in G$, $a.x = a.y \Rightarrow x = y$.
2) G *est régulier à droite c.-à-d.* $\forall a \in G$, $\forall x,y \in G$, $x.a = y.a \Rightarrow x = y$.
3) $\forall x,y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$ *et* $\left(x^{-1}\right)^{-1} = x$.
4) $\forall x \in G$, $\forall m,n \in \mathbb{Z}$, $x^{m+n} = x^m.x^n$ *et* $x^{mn} = (x^m)^n = (x^n)^m$.
5) $\forall x,y \in G$ *tel que* $xy = yx$, *on a :* $\forall n \in \mathbb{Z}$, $(xy)^n = x^n y^n$.

Remarque

Si la loi d'un groupe commutatif est notée additivement l'élément a^n (en notation multiplicative) sera noté par na, ainsi :

1) $(\forall a \in G)$, $0\ a = 0$, *(0 l'élément neutre de G).*
2) $(\forall a \in G)$, $(\forall n \in \mathbb{N})$, $na = a + a + \ldots + a$, (n *fois.*)
3) $(\forall a \in G)$, $(\forall n \in \mathbb{Z}^-)$, $na = (-n)(-a)$.
4) $(\forall x \in G)$, $(\forall n, m \in \mathbb{Z})$, $(m+n)x = mx + nx$ *et* $(mn)x = m(nx) = n(mx)$.
5) *Si G est commutatif, alors* $(\forall x, y \in G)$, $(\forall n \in \mathbb{Z})$, $n(x+y) = nx + ny$.

Définition

Soit $(G,.)$ *un groupe. On dit qu'une partie* H *de* G *est un sous-groupe de* G *si les conditions suivantes sont vérifiées :*

1) H *est stable par la loi "."*, *c.-à-d.* $\forall x,y \in H,\ x.y \in H$

2) $(H,.)$ *est un groupe*

Définition

Soit $(G,.)$ *un groupe. On dit qu'une partie* H *de* G *est un sous-groupe de* G *si les conditions suivantes sont vérifiées :*

1) H *est stable par la loi "."*, *c.-à-d.* $\forall x,y \in H,\ x.y \in H$

2) $(H,.)$ *est un groupe*

Théorème

Soit $(G,.)$ *un groupe d'élément neutre* e*. Pour qu'une partie* H *de* G *soit un sous-groupe de* G*, il faut et il suffit que :*

1) $H \neq \emptyset$ *;*

2) $\forall x,y \in H,\ xy^{-1} \in H.$

Preuve.

$\Rightarrow$) Trivial.
$\Leftarrow$) Supposons que $H \neq \emptyset$, $\forall x, y \in H,\ xy^{-1} \in H$ et montrons que $(H, \cdot)$ est un groupe.

- Comme $H \neq \emptyset$, alors H contient au moins un élément a, ainsi

$$aa^{-1} \in H, \quad \text{c.-à-d. } e \in H.$$

- Soit $a \in H$, alors $a^{-1} = ea^{-1} \in H$.
- Soient $a,\ b$ dans H, alors $a,\ b^{-1} \in H$, ainsi $ab = a(b^{-1})^{-1} \in H$, donc H est stable par la loi "$\cdot$".
- Soient $a,\ b,\ c$ dans H, alors $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ par l'associativité de la loi "$\cdot$" dans G et l'élément reste dans H par stabilité.

Donc H est un sous-groupe de G. 

Proposition

Soit $(G,.)$ *un groupe et* e *son élément neutre. Alors :*

1) $\{e\}$ *et* $\{G\}$ *sont des sous groupes de* G *;*
2) *Tout sous groupe de* G *contient* e *;*
3) *Si* $(H_i)_{i\in I}$ *est une famille de sous-groupes de* G*, alors* $\bigcap_{i\in I} H_i$ *est un sous-groupe de* G*.*

Proposition

Soit $(G,.)$ un groupe et e son élément neutre. Alors :

1) $\{e\}$ *et* $\{G\}$ *sont des sous groupes de* G *;*
2) *Tout sous groupe de* G *contient* e *;*
3) *Si* $(H_i)_{i\in I}$ *est une famille de sous-groupes de* G*, alors* $\bigcap_{i\in I} H_i$ *est un sous-groupe de* G*.*

Preuve.

Les assertions (1) et (2) sont évidentes.
(3) On a $H \neq \emptyset$ car $e \in \bigcap_{i\in I} H_i$. D'autre part, Soit $x,y \in \bigcap_{i\in I} H_i$, alors $(\forall\ i \in I),\ x,y \in H_i$, ainsi $(\forall\ i \in I),\ xy^{-1} \in H_i$, ce qui donne $xy^{-1} \in \bigcap_{i\in I} H_i$. Par suite $\bigcap_{i\in I} H_i$ est un sous groupe de G. □

Exemple

1) *On a* $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ *et chaque ensemble est un sous groupe, pour l'addition, de l'autre.*
2) *Soit* $(G,.)$ *un groupe, alors le centre de* G *définie par*

$$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$$

   est un sous-groupe de G*.*
3) *Soit* $(G,.)$ *un groupe, alors l'ensemble* $D(G)$ *des commutateurs de* G *définie par*

$$D(G) = \{[a,b] = aba^{-1}b^{-1} \mid a,b \in G\}$$

   est un sous groupe de G *appellé sous-groupe dérivé de* G*.*

Définition

Soit $(G,.)$ *un groupe et* A *une partie de* G*, alors l'intersection de tous les sous-groupes de* G *contenant* A *est un sous-groupe de* G*, appelé le sous-groupe engendré par* A *et est noté par* $\langle A \rangle$*.*

Définition

Soit $(G,.)$ un groupe et A une partie de G, alors l'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, appelé le sous-groupe engendré par A et est noté par $\langle A\rangle$.

Proposition

Soient $(G,.)$ un groupe et e son élément neutre. Alors

1) $\langle\emptyset\rangle = \{e\}$ *et* $\langle G\rangle = G$.

2) *Pour tout $x \in G$, le sous-groupe de G engendré par $\{x\}$ est donné par*

$$\langle x\rangle = \{x^n \,|\, n \in \mathbb{Z}\}.$$

3) *Soit A une partie de G, alors le sous-groupe de G engendré par A est donné par*

$$\langle A\rangle = \{x_1^{n_1}\ldots x_s^{n_s} \,|\, x_i \in A,\, 1 \leq i \leq s,\, n_i = \pm 1,\, s \in \mathbb{N}^*\}.$$

Preuve.

1) Puisque tous les sous-groupes de G contiennent l'élément neutre, on déduit facilement que $\langle\emptyset\rangle = \{e\}$. Aussi, comme le seul sous-groupe de G qui contient G c'est lui même, alors $\langle G\rangle = G$.

2) Posons $H = \{x^n \,|\, n \in \mathbb{Z}\}$, il est clair que H est un sous groupe de G contenant $\{x\}$. Donc $\langle x\rangle \subseteq H$ (car $\langle x\rangle$ est l'intersection de tous les sous groupes contenant x). D'autre part, Soit K un sous groupe de G contenant x, donc il contient tous les éléments de la forme x^n tel que $n \in \mathbb{Z}$, ainsi $K \supseteq H$. Donc l'intersection de tous les sous groupes de G contenant x, contient H, ce qui entraîne que $\langle x\rangle \supseteq H$ et Par conséquent $H = \langle x\rangle$.

3) On raisonne comme dans l'assertion (2). On pose

$$H = \{x_1^{n_1} \ldots x_s^{n_s} \,|\, x_i \in A,\, 1 \leq i \leq s,\, n_i = \pm 1,\, s \in \mathbb{N}^*\}$$

on vérifie facilement que H est un sous-groupe de G contenant A, alors il contient $\langle A\rangle$ (par définition). Et si K un sous groupe de G qui contient A, alors il va contenir H, ainsi l'intersection de tous les sous-groupe de G contenant A, contient H, ce qui veut dire $\langle A\rangle \supset H$. Donc $H = \langle A\rangle$.

□

Définition

Soit $(G,.)$ *un groupe. On dit que* $(G,.)$ *est un groupe monogène si* G *est engendré par un seul élément, c.-à-d.* $(\exists\ x \in G)$, $G = \langle x \rangle$. *Si de plus* $\mathrm{card}(G) = |G|$ *est fini, on dit que* G *est cyclique.*

Définition

Soit $(G,.)$ *un groupe. On dit que* $(G,.)$ *est un groupe monogène si* G *est engendré par un seul élément, c.-à-d.* $(\exists\, x \in G)$, $G = \langle x \rangle$. *Si de plus* $\mathrm{card}(G) = |G|$ *est fini, on dit que* G *est cyclique.*

Exemple

1) $(\mathbb{Z},+)$ *est un groupe monogène, et est engendré par* 1.
2) $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe cyclique d'ordre* n, *et est engendré par* $\overline{1}$.

Théorème

Soit $(G,.)$ *un groupe. Si* $(G,.)$ *est un groupe monogène, alors tous les sous-groupes de* G *sont monogène.*

Théorème

Soit $(G,.)$ un groupe. Si $(G,.)$ est un groupe monogène, alors tous les sous-groupes de G sont monogène.

Preuve.

On a G est monogène, donc $(\exists\ x \in G),\ G = \langle x \rangle$.
D'abord on a G et e sont monogène. Maintenant, Soit H un sous-groupe propre de G, c.-à-d. $H \neq G$ et $H \neq \{e\}$, donc il existe $a \in H$ tel que $a \neq e$. Comme $a \in G$, alors il existe $n \in \mathbb{Z}^*$ tel que $a = x^n$. Puisque $x^{-n} \in H$, on peut supposer que $n > 0$. Soit m le plus petit entier strictement positif tel que $x^m \in H$, donc $\langle x^m \rangle \subseteq H$. Soit $k \in \mathbb{N}^*$ tel que $x^k \in H$, effectuons la division euclidienne de k par m dans $\mathbb{Z}$, alors il existe $q, r \in \mathbb{Z}$ tel que $k = mq + r$ avec $0 \leq r < m$. Donc

$$x^k = x^{mq+r} = (x^m)^q x^r \Rightarrow x^r = x^k (x^m)^{-q} \in H,$$

ce qui entraîne que $r = 0$, car m est le plus petit. Ainsi $x^k = (x^m)^q$ est un élément du sous-groupe $\langle x^m \rangle$. Par conséquent $H = \langle x^m \rangle$, et donc H est monogène. □

Définition

1) *Soit* $(G,.)$ *un groupe fini, le nombre des éléments de* G *s'appel ordre de* G*, qu'on le note par* $\mathrm{ord}(G)$*,* $|G|$ *ou #* G *;*

2) *Soient* $(G,.)$ *un groupe fini et* e *son élément neutre, et soit* $a \in G$ *on appelle ordre de* a*, et on le note par* $\theta(a)$ *ou* $\mathrm{ord}(a)$*, le plus petit entier positif non nul,* n*, tel que* $a^n = e$*.*

Définition

1) *Soit* $(G,.)$ *un groupe fini, le nombre des éléments de* G *s'appel ordre de* G*, qu'on le note par* $\mathrm{ord}(G)$*,* $|G|$ *ou #* G *;*

2) *Soient* $(G,.)$ *un groupe fini et* e *son élément neutre, et soit* $a \in G$ *on appelle ordre de* a*, et on le note par* $\theta(a)$ *ou* $\mathrm{ord}(a)$*, le plus petit entier positif non nul,* n*, tel que* $a^n = e$*.*

Proposition

Soient $(G,.)$ *un groupe fini et* e *son élément neutre, alors pour tout* $a \in G$ *on a* $\theta(a) = |\langle a \rangle|$*.*

Preuve.

Notons par $n = \theta(a)$. On a : $\langle a \rangle = \{\ldots, a^{-(n+1)}, a^{-n}, \ldots, a^{-1}, e, a, \ldots, a^n, a^{n+1}, \ldots\}$.
Si $m \in \mathbb{Z}$ tel que $|m| \geq n$, il existe $q, r \in \mathbb{Z}$ tel que $m = nq + r$ où $0 \leq r < n$, donc

$$a^m = (a^n)^q a^r = a^r,$$

on en déduit que

$$\langle a \rangle = \{a^{-(n-1)}, \ldots, a^{-1}, e, a, \ldots, a^{n-1}\}.$$

D'autre part, si k est un entier relatif tel que $-(n-1) \leq k \leq -1$, alors $a^k = a^{n+k}$, de plus $1 \leq n+k \leq (n-1)$ c.-à-d. pour chaque k tel que $-(n-1) \leq k \leq -1$, il existe k' tel que $1 \leq k' \leq (n-1)$ et $a^k = a^{k'}$, ainsi

$$\langle a \rangle = \{e, a, \ldots, a^{(n-1)}\}.$$

Or pour tout k, k' tel que $1 \leq k, k' \leq (n-1)$ et $k \neq k'$ on a $a^k \neq a^{k'}$, car sinon

$$a^k = a^{k'} \Longrightarrow a^{k-k'} = e \Longrightarrow (k-k') \in \{0, n\},$$

ce qui n'est pas le cas. Par conséquent $|\langle a \rangle| = n$. □

Définition

Soient $(G,.)$ *un groupe et* H *un sous groupe de* G*. Alors* H *est dit sous-groupe distingué (ou normal) dans* G *et on écrit* $H \lhd G$ *si*

$$(\forall\ x \in G),\ xHx^{-1} = H, (\text{ ou } xH = Hx).$$

Définition

Soient $(G,.)$ *un groupe et* H *un sous groupe de* G. *Alors* H *est dit sous-groupe distingué (ou normal) dans* G *et on écrit* $H \lhd G$ *si*

$$(\forall\ x \in G),\ xHx^{-1} = H, (\text{ ou } xH = Hx).$$

Remarque

Soit G *un groupe abélien, alors tous les sous-groupes de* G *sont distingués dans* G.

Définition

Soit $(G,.)$ *un groupe et* H *un sous groupe de* G*. On appelle congruence à droite (resp. à gauche) modulo* H*, la relation définie sur* G *par :*

$$x\mathcal{R}_d y \Longleftrightarrow xy^{-1} \in H \ (\text{resp. } x\mathcal{R}_g y \Longleftrightarrow x^{-1}y \in H).$$

Remarque

Les relations $\mathcal{R}_d$ et $\mathcal{R}_g$ sont des relations d'équivalences dont les ensembles quotients respectifs sont notés $(G/H)_d$ et $(G/H)_g$ avec

$$(G/H)_d = \{Hx \,|\, x \in G\} \text{ et } (G/H)_g = \{xH \,|\, x \in G\}.$$

De plus, Pour $x \in G$, l'application $H \to Hx$ (resp. $H \to xH$) définie par $x \mapsto hx$ (resp. $x \mapsto xh$) est une bijection. Par conséquent toutes les classes d'équivalence à gauche (resp. à droite) ont le même cardinal égal à celui de H.
Si $H \lhd G$, alors les deux ensembles $(G/H)_d$ et $(G/H)_g$ coincident, et on note G/H. De plus G/H muni de la multiplication induite par celle de G définie par

$$\overline{x}.\overline{y} = \overline{x.y},$$

est un groupe appelé groupe quotiont de G par H.

Théorème (Théorème de Lagrange)

Soient $(G,.)$ *un groupe fini et* H *un sous-groupe de* G*, alors l'ordre de* H *divise l'ordre de* G*. Plus précisement on a :*

$$|G| = |H||(G/H)_g| = |H||(G/H)d|$$

Théorème (Théorème de Lagrange)

Soient $(G,.)$ un groupe fini et H un sous-groupe de G, alors l'ordre de H divise l'ordre de G. Plus précisement on a :

$$|G| = |H||(G/H)_g| = |H||(G/H)d|$$

Preuve.

Ecrivons le groupe G comme réunion disjointe des classes d'equivalences de $(G/H)_g$, donc

$$|G| = \sum_{\bar{x}\in(G/H)_g} |\bar{x}|,$$

et comme $\bar{x} = xH$ est en bijection avec H, alors

$$|G| = \sum_{\bar{x}\in(G/H)_g} |H| = |(G/H)_g||H| = |(G/H)_d||H|.$$



Définition

Soient $(G,.)$ *un groupe et* H *un sous groupe de* G*. L'indice de* H *dans* G*, noté* $[G:H]$ *est le cardinal de* $(G/H)_g$ *qui est égal à celui de* $(G/H)_d$ *et on a* $[G:H] = |(G/H)_g| = |(G/H)_d|$*.*

Définition

Soient $(G,.)$ *un groupe et* H *un sous groupe de* G*. L'indice de* H *dans* G*, noté* $[G:H]$ *est le cardinal de* $(G/H)_g$ *qui est égal à celui de* $(G/H)_d$ *et on a* $[G:H] = |(G/H)_g| = |(G/H)_d|$*.*

Proposition

Soit $(G,.)$ *un groupe fini d'élément neutre* e*. Si* G *est d'ordre un nombre premier* p *alors* G *est cyclique.*

Définition

Soient $(G,.)$ *un groupe et* H *un sous groupe de* G*. L'indice de* H *dans* G*, noté* $[G:H]$ *est le cardinal de* $(G/H)_g$ *qui est égal à celui de* $(G/H)_d$ *et on a* $[G:H] = |(G/H)_g| = |(G/H)_d|$*.*

Proposition

Soit $(G,.)$ *un groupe fini d'élément neutre* e*. Si* G *est d'ordre un nombre premier* p *alors* G *est cyclique.*

Preuve.

On suppose que le groupe G est d'ordre un nombre premier p, donc $|G| = p > 1$, ainsi G contient un élément a distinct de e. Posons $H = \langle a \rangle$, on a H est un sous groupe de G, tel que $|H| > 1$, par le théorème de Lagrange on tire que $|H| | p$ ce qui implique que $|H| = p$, car p est premier, ce qui donne que $G = H = \langle a \rangle$. □

Définition

Soient $(G_1, .)$ *et* $(G_2, *)$ *deux groupes. Un homomorphisme de* G_1 *dans* G_2 *est une application* $f : G_1 \to G_2$ *telle que :*

$$\forall\ x, y \in G_1,\ \ f(x.y) = f(x) * f(y).$$

Si de plus l'homomorphisme f *est bijectif, on dit que* f *est un isomorphisme de* G_1 *dans* G_2 *ou que* G_1 *est isomorphe à* G_2 *et on écrit* $G_1 \simeq G_2$

Propriétés

Soient $(G_1,.)$ *et* $(G_2,.)$ *deux groupes d'éléments neutres respectifs* e_1 *et* e_2, *et soit* $f: G_1 \to G_2$ *un homomorphisme, alors :*

1) $f(e_1) = e_2$

2) $\forall x \in G_1,\ f(x^{-1}) = (f(x))^{-1}$

Propriétés

Soient $(G_1, .)$ *et* $(G_2, .)$ *deux groupes d'éléments neutres respectifs* e_1 *et* e_2*, et soit* $f : G_1 \to G_2$ *un homomorphisme, alors :*

1) $f(e_1) = e_2$
2) $\forall x \in G_1,\ f(x^{-1}) = (f(x))^{-1}$

Preuve.

1) On a $f(e_1).e_2 = f(e_1) = f(e_1.e_1) = f(e_1).f(e_1)$, or G est régulier à gauche, donc on en déduit que $f(e_1) = e_2$.
2) On a $f(x^{-1}).f(x) = f(x^{-1}.x) = f(e_1) = e_2$, donc $f(x^{-1}) = (f(x))^{-1}$.



Proposition

Soient $(G_1, .)$, $(G_2, .)$ *et* $(G_3, .)$ *trois groupes. Alors*

1) *Si* $f : G_1 \to G_2$ *et* $g : G_2 \to G_3$ *des homomorphismes de groupes, alors la composée* $g \circ f : G_1 \to G_3$ *est un homomorphisme de groupe ;*
2) *Si* $f : G_1 \to G_2$ *est un isomorphisme de groupe, alors* $f^{-1} : G_2 \to G_1$ *l'est aussi.*

Proposition

Soient $(G_1,.), (G_2,.)$ *et* $(G_3,.)$ *trois groupes. Alors*

1) *Si* $f : G_1 \to G_2$ *et* $g : G_2 \to G_3$ *des homomorphismes de groupes, alors la composée* $g \circ f : G_1 \to G_3$ *est un homomorphisme de groupe ;*
2) *Si* $f : G_1 \to G_2$ *est un isomorphisme de groupe, alors* $f^{-1} : G_2 \to G_1$ *l'est aussi.*

Preuve.

1) Découle facilement de la definition
2) Soient $y_1, y_2 \in G_2$, alors il existe $x_1, x_2 \in G_1$ uniques tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$, ainsi $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$. D'autre part, on a

$$f^{-1}(y_1.y_2) = f^{-1}(f(x_1).f(x_2)) = f^{-1}(f(x_1.x_2)) = x_1.x_2 = f^{-1}(y_1).f^{-1}(y_2),$$

ainsi f^{-1} est un homomorphisme et comme il est bijectif, alors f^{-1} est un isomorphisme.



Proposition

Soient $(G_1,.), (G_2,.)$ *deux groupes d'éléments neutres respectifs* e_1 *et* e_2 *et* $f : G_1 \to G_2$ *un homomorphisme de groupes alors*

1) f *est injectif si et seulement si* $\text{Ker}(f) = \{e_1\}$, *avec*

$$\text{Ker}(f) = \{x \in G_1 \,|\, f(x) = e_2\} \ (\textit{noyau de } f);$$

2) f *est surjectif si et seulement si* $\text{Im}(f) = G_2$, *avec*

$$\text{Im}(f) = \{f(x) \,|\, x \in G_1\} \ (\textit{Image de } f);$$

3) $\text{Ker}(f)$ *et* $\text{Im}(f)$ *sont des sous groupes de* G_1 *et* G_2 *respectivement ;*

4) $\text{Ker}(f)$ *est un sous groupe distingué dans* G_1 *et on a*

$$G_1/\text{Ker}(f) \simeq \text{Im}(f) \ (\textbf{Premier théorème d'isomorphisme}).$$

Preuve

1) Soit $x, y \in G_1$, on a

$$f(x) = f(y) \Leftrightarrow f(x^{-1}y) = e_2 \Leftrightarrow x^{-1}y \in \mathrm{Ker}\,(f).$$

Donc si $\mathrm{Ker}\,(f) = \{e_1\}$ alors $f(x) = f(y) \Rightarrow x = y$, ainsi f est injectif. Réciproquement, supposons que f est injectif. Soit $x \in \mathrm{Ker}\,(f)$, alors $f(x) = e_2 = f(e_1)$, or f est injectif, donc on déduit que $x = e_1$. Ainsi $\mathrm{Ker}\,(f) = \{e_1\}$.

2) La definition de la surjection.

3) Découle facilement de la définition.

Preuve

4) Soit $y \in \text{Ker}(f)$, alors pour tout $x \in G_1$ on a

$$f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)e_2f(x^{-1}) = f(x)f(x^{-1}) = f(x)(f(x))^{-1} = e_2,$$

donc

$$x\text{Ker}(f)x^{-1} = \text{Ker}(f), \quad \text{c.-à-d. } \text{Ker}(f) \lhd G_1.$$

Posons :

$$\begin{array}{llll} \overline{f}: & G_1/\text{Ker}(f) & \Longrightarrow & \text{Im}(f) \\ & \bar{x} & \longmapsto & \overline{f}(\bar{x}) = f(x) \end{array}.$$

$\overline{f}$ est bien définie et est un homomorphisme bijectif car

$$\bar{y} = \bar{x} \Leftrightarrow xy^{-1} \in \text{Ker}(f) \Leftrightarrow f(xy^{-1}) = e_2 \Leftrightarrow f(x) = f(y) \Leftrightarrow \overline{f}(\bar{x}) = \overline{f}(\bar{y}).$$

Donc $\overline{f}$ est bien définie et est injectif et comme elle est surjectif (par construction), elle est bijectif.
On vérifie facilement que $\overline{f}$ est un homomorphisme, donc $\overline{f}$ est un isomorphisme.

Exemple

Soit $(G,.)$ *un groupe.*

1) *Soit* $a \in G$*, alors l'application* $(\mathbb{Z},+) \to (G,.)$ *définie par* $n \mapsto a^n$ *est un homomorphisme de groupe.*

2) *Soit* $a \in G$*, alors l'application* $x \mapsto a^{-1}xa$ *définie de* G *dans* G *est un automorphisme (endomorphisme bijectif) et son automorphisme réciproque est* $x \mapsto axa^{-1}$*. Les automorphismes de ce type s'appellent les automorphismes intérieurs de* G*. Leur ensemble noté* $\mathrm{Int}(G)$ *est un sous-groupe du groupe des automorphisme de* G*,* $\mathrm{Aut}(G)$*, pour la loi de composition d'application "*$\circ$*".*

3) *Si on note par* Θ_a *l'automorphisme intérieur* $x \mapsto axa^{-1}$*, alors l'application*

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Int}(G) \\ a & \longmapsto & \Theta_a \end{array}$$

est un homomorphisme de groupes.

Proposition

1) *Tout groupe d'élement neutre e, engendré par deux élément x et y distincts de e tel que*

$$x^3 = y^2 = (xy)^2 = e$$

est isomorphe à $\mathcal{S}_3$ (le groupe des bijection de $\{1,2,3\}$ vers lui même).

2) *Si G est un groupe engendré par deux élément $x \neq e$ et $y \neq e$ tel que*

$$x^2 = y^2 = (xy)^3 = e,$$

alors G est isomorphe à $\mathcal{S}_3$ ou G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Preuve

1) Soit G un tel groupe, un élément de G s'écrit comme produit d'un nombre fini de x et y, et dans ce produit on peut remplacer x^3, y^2 et $xyxy$ par e, ceci par hypothèse.

Mais on a aussi :

$$xyxy = e \Rightarrow xy = x^{-1}y^{-1} = x^2y,$$

et

$$yxy = x^2y^2 = x^2, \ yxyx = e,$$

aussi

$$xyx = x^3y = y \text{ et } yx^2 = x^2yx = x^4y = xy,$$

donc

$$xyx^2 = x^2y \text{ et } x^2yx = x^4y = xy.$$

Donc les produits de quatre facteurs se ramènent à un produit d'au plus trois facteurs et finalement à l'un des termes e, x, x^2, y, xy, x^2y.

De plus si $x \neq e$ et $x^3 = e$, l'élémnt x est d'ordre 3 et y est d'ordre 2. Ainsi le groupe G a un ordre multiple de 6, il est donc d'ordre 6. Comme il est non commutatif il est isomorphe à $\mathcal{S}_3$, (pour contruire l'isomorphisme il suffit de considérer $\mathcal{S}_3 = \langle (1,2,3), (1,2) \rangle$, et l'image de x c'est le cycle $(1,2,3)$ et celui y est la transposition $(1,2)$).

Preuve

2) Posons $z = xy$, donc

$$(zy)^2 = (xy^2)^2 = x^2 = e,$$

puisque $x = zy$, on est ramené au premier cas. Donc le groupe engendré par x et y est celui engendré par z et y vérifiant

$$z^3 = y^2 = (zy)^2 = e.$$

On en déduit que si $z \neq e$ alors G est isomorphe à $\mathcal{S}_3$. Sinon $x = y$ et on a G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.